Elektronische Zustellung Abholung von Zustellung über E-mail Clients	Konvention zusemail-1.4.0 Ergebnis der AG

Kurzbeschreibung	Um die Verbreitung der elektronischen Zustellung weiter zu forcieren, soll der Zugang zu den Zustellstücken auch auf alternative Wege wie bspw. über E-Mailzugänge ermöglicht werden. Besonders in Hinblick auf „Großkunden“, d.h. Empfänger mit einem großen Aufkommen von Zustellstücken wie Firmen oder auch Behörden (sofern Behörden Zustellungen gem. den Möglichkeiten des AVG auch annehmen), wäre ein Mailzugang ein entsprechender Mehrwert. Aber auch für herkömmliche Empfänger ist der für sie gewohnte Zugang via E-Mail-Client sehr attraktiv.	
Autor(en):	Reinhard Posch Thomas Rössler	Projektteam / Arbeitsgruppe: AG-ZUSE / AG-II
Beiträge von:	Arne Tauber, Peter Reichstädter	

Version 1.4.0 : **02.02.2012**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Unter-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Detail-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Anmerkungen:	*(Detailangaben zur Freigabe)*

Inhaltsverzeichnis

1. Einleitung

Um die Verbreitung der elektronischen Zustellung weiter zu forcieren, soll der Zugang zu den Zustellstücken auch auf alternative Wege, wie bspw. über E-Mailzugänge, ermöglicht werden. Besonders in Hinblick auf „Großkunden“, d.h. Empfänger mit einem großen Aufkommen von Zustellstücken wie Firmen oder auch Behörden (sofern Behörden Zustellungen gem. den Möglichkeiten des AVG auch annehmen), wäre ein Mailzugang ein entsprechender Mehrwert. Aber auch für herkömmliche Empfänger ist der für sie gewohnte Zugang via E-Mail-Client sehr attraktiv.

Dieses Dokument definiert eine grundsätzliche technische Art der Annahme von Zustellstücken nach §35(3) [ZustG07] unter Verwendung von SSL-Clientzertifikaten. Es soll den Zustelldienstbetreibern Anhaltspunkte liefern, wie sie diese für ihre Kunden alternative Zugangsform vor dem Hintergrund der aktuellen Rechtslage bereitstellen können.

Die vorgestellte Art der Abholung entspricht einer Abholung auf Basis einer besonderen Vereinbarung (gem. §35(3) [ZustG07]) und erfordert die Abholung von Zustellstücken unter Verwendung eines (SSL-)Client-Zertifikates, wodurch im täglichen Umgang mit der Zustellung jede weitere Interaktion mit dem Zustelldienst unter Verwendung der Bürgerkarte entfällt. Der Zustellnachweis erfolgt dabei mit der „Technologie der Signatur“ beim Zugang mit Clientzertifikat (SSL) implizit (im Zuge des SSL-Handshakes). Dieser Vorgang wird vom Zustelldienst protokolliert (Zeitpunkt, Zertifikat, Gültigkeit); als Annahmezeitpunkt der Zustellung gilt der protokollierte Zeitpunkt der Authentifikation (SSL-Handshake). Langen während einer zertifikatsaktivierten E-Mail-Client-Session (IMAP) weitere Zustellstücke ein, so werden diese erst nach erneutem SSL-Verbindungsaufbau (erneutem Handshake) und damit Zustellnachweis als E-Mail übermittelt.

Nachfolgend wird das Kernprinzip zur Verwendung mit einem E-Mail-Client definiert.

2. Abholung mit automatischer Signatur

Paragraph §35 (3) ZustG [1] sieht vor, dass die Abholung von Zustellstücken beim Zustelldienst auf Basis einer besonderen Vereinbarung zwischen Zustelldienst und Empfänger auch mittels automatisch ausgelöster Signaturen möglich ist.

Auszug §35 (3) [ZustG07]

> *[..] (3) Der Zustelldienst hat sicherzustellen, dass zur Abholung bereitgehaltene Dokumente nur von Personen abgeholt werden können, die zur Abholung berechtigt sind und ihre Identität und die Authentizität der Kommunikation mit der Bürgerkarte (§ 2 Z 10 E-GovG) nachgewiesen haben. Zur Abholung berechtigt sind der Empfänger und, soweit dies von der Behörde nicht ausgeschlossen worden ist, eine zur Empfangnahme bevollmächtigte Person. Identifikation und Authentifizierung können auf Grund einer besonderen Vereinbarung des Empfängers mit dem Zustelldienst auch durch eine an die Verwendung sicherer Technik gebundene automatisiert ausgelöste Signatur erfolgen. Der Zustelldienst hat alle Daten über die Verständigungen gemäß Abs. 1 und 2 und die Abholung des Dokuments zu protokollieren und der Behörde unverzüglich zu übermitteln; die Gesamtheit dieser Daten bildet den Zustellnachweis. [..]*

Diese Formulierung des Zustellgesetzes stellt auf eine eindeutige und hinreichend sichere Authentifikation des Empfängers ab, was – nach Zustimmung des Empfängers bzw. auf Basis einer besonderen Vereinbarung – auch unter Verwendung eines Client-Zertifikates technisch ermöglicht wird. Konkret wird ein SSL-Clientzertifikat dazu verwendet, um eine sichere Verbindung zum Zustellserver aufzubauen, und anhand dessen, im Zuge des Verbindungsaufbaus, eine Identifikation und Authentifikation (technisch auf Basis einer Signatur) des Gegenübers erfolgt. Grundvoraussetzung dafür ist allerdings, dass eine erstmalige Anmeldung am Zustelldienst unter Verwendung der Bürgerkarte des Empfängers erfolgte (§33 (1) [ZustG07]), und diese besondere Form der Authentifikation vereinbart (in einem separaten Sub-Menü im Menü „Einstellungen“ des Web-Frontend des Zustelldienstes). Das Client-Zertifikat sollte zeitlich nur begrenzt gültig sein (bspw. maximal 6 Monate) und muss dann wieder unter Verwendung der Bürgerkarte erneuert werden.

Erfolgt die Abholung der Zustellstücke über eine nach diesem Prinzip authentifizierten Verbindung, so können Zustellstücke unmittelbar und ohne weiteres Zutun seitens des Empfängers bezogen werden, bspw. über gängige Mail-Protokolle (IMAP). Der Zustelldienst ist allerdings dazu angehalten, einen derart erfolgten Verbindungsaufbau mit Signaturtechnologie (SSL) zur Abholung von Zustellstücken geeignet und nachhaltig als Zustellnachweis zu protokollieren. Es muss vor allem aus den Aufzeichnungen des Zustelldienstes erkennbar sein, ob und welche Zustellstücke nach Authentifikation mit der Bürgerkarte oder im Wege der besonderen Vereinbarung mittels Client-Zertifikat abgeholt wurden, und zu welchem Zeitpunkt der Zustellnachweis erfolgt hat.

Der Zustellnachweis erfolgt mit der „Technologie der Signatur“ beim Zugang mit Clientzertifikat (SSL) implizit; dieser Vorgang muss vom Zustelldienst protokolliert (Zeitpunkt, Zertifikat, Gültigkeit) werden. Langen während einer zertifikatsaktivierten E-Mail-Client-Session weitere Zustellstücke ein, so werden diese erst nach erneutem SSL-Verbindungsaufbau (erneutem Handshake) und damit Zustellnachweis als E-Mail übermittelt.

Die Zustellung mit automatischer Signatur sieht keine Vollmachten vor. Es ist daher für den tatsächlichen Empfänger (z.B. Firma) ein derartiges Zertifikat zur automatischen Signatur zu verwenden.

Der Gesamtprozess gliedert sich in eine Registrierungsphase und eine Abholphase. Beide Phasen werden nachfolgend im Detail spezifiziert.

2.1. Registrierungsphase

Die Registrierungsphase im Überblick:

1. Der Empfänger muss sich zur Abholung per automatischer Signatur durch einen entsprechenden Menüpunkt (Sub-Menü im Bereich „Einstellung“) am Zustelldienst registrieren. Bei dieser Registrierung trifft der Empfänger die besondere Vereinbarung zur Abholung seiner Zustellstücke, im Sinne §35(3) ZustG. Zur Zustimmung wird dem Empfänger ein Formular zur elektronischen Signatur mit der Bürgerkarte vorgelegt. Das durch den Bürger signierte Stück muss vom Zustelldienst evident gehalten werden.

   Der Zustelldienst stellt zur Registrierung einen eigenen Menüpunkt im Bereich „Einstellungen“ zur Verfügung.

2. Im Verlauf der Registrierung werden dem Empfänger durch den Zustelldienst Mailkonto-Einstellungen mitgeteilt, anhand der der Empfänger auf seinen persönlichen Briefkasten per E-Mail-Protokoll zugreifen kann. Die Daten sind:

   a) ein Kontoname in Form einer E-Mail-Adresse, z.B.: FBNR4711@zustellung.gv.at; diese ist nicht eine E-Mail-Adresse im herkömmlichen Sinn und kann auch nicht zum Senden und Empfangen von herkömmlichen E-Mails verwendet werden. Sie dient lediglich als Vehikel zur eindeutigen Identifikation des zugehörigen Mail- bzw. Zustellkontos.

   b) (optional) Zugangspasswort

   c) Da die Verbindung clientseitig über ein SSL-Zertifikat authentifiziert wird, kommt dem Zugangspasswort keine besondere Bedeutung bei. Aus sicherheitstechnischer Sicht tritt anstelle des Zugangspasswortes das SSL-Zertifikat zur Clientauthentifizierung. Auf ein Postfach darf nur jener Anwender Zugriff bekommen, der sich mit dem dazu registrierten SSL-Zertifikat authentifiziert hat (siehe Punkt 3 der Registrierung).

   d) Zugangsdaten zum Zustelldienst in Form von Mail-Server Parametern

   e) das vom Server Verwendete SSL-Zertifikat (zur Server-Authentifikation) (Abholung erfolgt in der durch MOA-ID und SSL/TLS-gesicherten Verbindung der Session des Zustellservers)

   f) Belehrung über die sorgfältige Verwendung und den Widerruf.

3. Um zu gewährleisten, dass letztlich auch nur der tatsächliche Empfänger auf den Briefkasten zugreifen kann, ist der Zugriff via E-Mail-Protokolle durch ein Client-Zertifikat abzusichern (SSL-Client Zertifikat). Letztlich autorisiert dieses Client-Zertifikat den verwendeten (E-Mail-)Client zur automatischen Abholung der Zustellstücke. Dieses Client-Zertifikat wird für den Empfänger im Zuge der Registrierung ausgestellt, das dieser dann in seinem E-Mail-Client – oder auch Web-Browser – zur Client-Authentifikation als Alternative zur Bürgerkarte verwenden kann. Die Zeitspanne der Gültigkeit dieses Zertifikates muss durch den Benutzer selbst gewählt werden können (maximale Zeit ist ein Konfigurationsparameter; eine sinnvolle maximale Gültigkeitsdauer ist 6 Monate; nachdem das Zertifikat zeitlich abgelaufen ist, muss der Anwender dieses unter Verwendung seiner Bürgerkarte erneuern). Zudem muss das Zertifikat einen Identifikationsbegriff enthalten, anhand dessen die Zugehörigkeit des Zertifikates zum jeweiligen Zustellkonto eindeutig feststellbar ist (stellt die exklusive Bindung eines SSL-

Zertifikates an ein Zustellkonto dar). Als Identifikationsbegriff ist die vom Zustelldienst für den Empfänger vergebene E-Mail-Adresse (zum Beispiel: max.mustermann@zustellung.gv.at) im Subject (CN) des Zertifikates zu verwenden. Variationen der Zertifikatsausstellung sind im Punkt 4 beschrieben (siehe b): i – iii).

Das Client-Zertifikat ist ein gewöhnliches SSL-Zertifikat zur Client-Authentifizierung. Die technische Qualität des Client-Zertifikates in Bezug auf die zu verwendenden, kryptographischen Algorithmen soll dem eines qualifizierten Zertifikats entsprechen (gem. den zum Zeitpunkt der Ausstellung anzuwendenden Vorgaben – siehe [SigG07] und [SigV07]). Auf die technische Unterstützung der verwendeten Algorithmen bei den verschiedenen Clients und Betriebssystemen ist zu achten. Vorbedingung für die Ausstellung des Zertifikates ist die unmittelbar zuvor erfolgte Identifikation und Authentifikation des Antragsstellers unter Verwendung dessen Bürgerkarte. Die Ausstellung des Zertifikates nimmt der Zustelldienst selbst vor (ausgenommen hiervon die Ausstellung nach der optionalen Variante b/iii – siehe Punkt 4). Die vom Zustelldienst zur Ausstellung verwendeten Schlüssel und Zertifikatshierarchien (CA-Zertifikate und -Schlüssel) sind ausschließlich für den Zweck der Erstellung von Client-Zertifikaten in dem in diesem Dokument spezifizierten Sinn zu verwenden.

4. Der Zustelldienst darf so nur jenem Client Zugang zu dem Inhalt eines Briefkasten gewähren, wenn dieser – neben den herkömmlichen Zugangsdaten (wie im Falle des E-Mail-Zugangs: E-Mail-Adresse und ggf. Zugangspasswort) – auch das zum Zustellkonto registrierte Client-Zertifikat vorweisen kann. Es soll dabei möglich sein, dass ein Anwender auch mehrere Client-Zertifikate für sein Zustellkonto beantragen kann, um so auch mehrere (E-Mail-)Clients damit ausstatten zu können. Nicht zuletzt dazu soll dem Anwender im Rahmen seiner Zustellkontokonfigurationen ein rudimentäres Zertifikatsmanagement zur Verfügung gestellt werden, anhand dessen er bei Bedarf neue Zertifikate generieren oder aber auch alte Zertifikate löschen (widerrufen) kann. Ein derartiges Zertifikatsmanagement-Interface soll daher die folgenden Funktionalitäten bieten:

   a) Auflistung registrierter Client-Zertifikate

   b) (Neu-)Ausstellung/Registrierung eines (weiteren) Client-Zertifikates mit der Bürgerkarte:

      i) *Ausstellungsvariante 1*: privater Schlüssel zur Client-Authentifizierung wird direkt im Browser des Anwenders erzeugt und das erstellte Zertifikat unmittelbar im Zertifikatsspeicher des Browsers abgelegt wird (z.B. via ActiveX)

      ii) *Ausstellungsvariante 2*: privater Schlüssel wird seitens Zustelldienst erzeugt und das Zertifikat samt Schlüsselpaar als PKCS#12-Datei zum lokalen abspeichern angeboten

      iii) *Ausstellungsvariante 3 (optional)*: Anwender bringt bestehendes, extern generiertes Zertifikat bei und registriert dieses zum Zustellkonto. In dieser Ausstellungsvariante muss der Fingerprint des Zertifikates als Identifikationsbegriff herangezogen werden.

   c) Widerruf/Löschen eines bestehenden Client-Zertifikates

2.2. Abholphase

Die Abholphase unter Verwendung eines E-Mail-Clients im Überblick:

1. Gelangt ein neues Zustellstück in den Briefkasten des Empfängers, so wird dieser über die bekannten Mechanismen und Verständigungsadressen darüber informiert.

2. Auf Basis der besonderen Vereinbarung, sind alle neu eingelangten Zustellstücke ab dem nächsten SSL-Sessionaufbau (dies entspricht dem Zustellnachweis) per E-Mail-Protokoll abholbar, sofern der verwendete E-Mail-Client das registrierte Client-Zertifikat zur Authentifikation gegenüber dem Mailserver-Dienst des Zustelldienstes verwendet (es muss sichergestellt werden, dass ausschließlich die zu dem jeweiligen Zustellkonto registrierten Client-Zertifikate für den Zugriff darauf verwendet werden können; ein Zugriff unter Verwendung eines mit einem anderen Zustellkonto verknüpften Client-Zertifikats darf nicht möglich sein). Das heißt, der Zustelldienst verteilt jedes Zustellstück nach dessen einlangen auch über den E-Mail-Zugang des Zustellkontos, sobald das Zustellstück explizit via Bürgerkarte oder implizit via Client-Authentifizierung nachweislich angenommen wurde. Der Zustelldienst muss Aufzeichnungen und Protokolldaten der Anmeldung – Identifikation und Authentifikation des E-Mail-Clients unter Verwendung eines registrierten Client-Zertifikates – evident halten, um bei Bedarf den korrekten Abholvorgang belegen zu können. Es muss außerdem aus den Aufzeichnungen des Zustelldienstes heraus klar erkennbar sein, welche Zustellstücke durch explizite Abholung, das heißt unter Verwendung der Bürgerkarte, und welche implizit unter Verwendung eines Client-Zertifikates in Empfang genommen worden sind. Der Empfänger bekommt so letztlich unmittelbar alle Zustellstücke in seinem E-Mail-Client dargestellt (je nach verwendetem E-Mail-Protokoll – z.B. IMAP – sofort oder auf Anfrage).

3. Wurde seitens Zusteller ein Zustellnachweis angefordert, so wird dieser vom Zustelldienst unter Angabe des Zeitpunktes des SSL-Sessionaufbaus erzeugt, signiert und an den Zusteller retourniert. Aus dem Text der Empfangsbestätigung muss der Umstand einer Abholung auf Basis §35 (3) ZustG erkennbar sein.

2.3. Erläuterungen und Ergänzungen

Diese Lösung ist aus rechtlicher Sicht konform mit der Abholung auf Basis einer besonderen Vereinbarung wie in §35(3) [ZustG07] vorgesehen.

Aus technischer Sicht erscheint die Lösung attraktiv – besonders aufgrund der minimalen Anforderungen an die Empfängerseite, da der Empfänger neben seinem E-Mail-Client keinerlei zusätzlicher Softwarekomponenten benötigt, sofern dieser die Authentifikation per Client-Zertifikat unterstützt. Jedoch auch auf Seiten des Zustelldienstes ist das Bereitstellen der Zustellstücke über E-Mail-Protokolle mit Standard-Serversoftwarelösungen und vertretbaren Aufwand bewerkstelligbar. Die Annahme der Zustellstücke unter Anwendung eines Client-Zertifikates tritt anstelle der expliziten Annahme mit der Bürgerkarte. Als Annahmezeitpunkt gilt der Zeitpunkt der Authentifikation mit einem registrierten Client-Zertifikat (Zeitpunkt des SSL-Handshakes).

Verwendet der E-Mail-Client des Empfängers eine Client-Authentifizierung unter Anwendung des registrierten Client-Zertifikates, so gelten alle bis zum Zeitpunkt des SSL-Handshakes eingelangten, neuen Zustellstücke als angenommen, mit dem protokollierten Zeitpunkt der Client-Authentifizierung (SSL-Handshake) als Annahmezeitpunkt. Ab diesem Zeitpunkt werden neue Zustellstücke auch für den Zugang via Mail-Protokoll freigegeben. Erfolgt diese Art der Authentifizierung bei jedem Verbindungsaufbau durch den Mail-Client selbst, so ist eine möglichst transparente Abholung von neuen Zustellstücken möglich.

Um ungeachtet des vom Anwender eingesetzten E-Mail-Clients diese Art des Zugriffs zu ermöglichen, kann eine entsprechende Client-Komponenten zur zertifikatsbasierten Client-Authentifizierung durch den Zustelldienstbetreiber bereitgestellt werden. Eine Variante einer solchen Client-Komponente ist eine lokale Authentifizierungskomponente, die in Richtung

Zustelldienst das ausgestellte Client-Zertifikat zur Authentifikation verwendet und in Richtung lokalem E-Mail-Client als Proxy fungiert. In diesem Szenario verbindet sich daher der lokale E-Mail-Client des Anwenders mit der lokalen Authentifizierungskomponente, die sich selbst, unter Verwendung des Client-Zertifikates, mit dem eigentlichen Mail-Zugang zum Zustellserver verbindet.

Da der Zustelldienst technisch einen E-Mail-Dienst bereitstellt, muss dem Empfänger zweifelsfrei bekannt gemacht werden, wie lange Zustellstücke am Server nach dem ersten Abruf vorgehalten bleiben (im Einklang mit den anzuwendenden Rechtsnormen). Besonders bei Bezug der Zustellstücke über IMAP ist durch das damit verbundene Anwenderverhalten eine längere Vorhaltefrist der Zustellstücke am Server anzunehmen. Der Zustelldienstbetreiber hat seine Kunden entsprechend zu informieren; das Löschen von Zustellstücken durch den Zustelldienst muss dem Anwender (Kunden) zuvor angekündigt werden.

Zusätzlich zum Zugang via E-Mail-Protokolle muss auf gleiche Weise – unter Anwendung einer automatisiert ausgelösten Signatur – der direkte Zugang zu den Zustellstücken via Web-Browser angeboten werden. Das heißt, dass ein Web-Browser, der sich eines registrierten Client-Zertifikates zur Client-Authentifizierung bedient, sofort und unmittelbar Zugang zu den Zustellstücken bekommt (via Web-Interface des Zustelldienstes). Es gelten die Definitionen des Abholprozesses nach Abschnitt 2.2 sinngemäß. Somit wird erreicht, dass ein Anwender ein Client-Zertifikat wie in Abschnitt 2 beschrieben ausgestellt bekommt, dieser dieses dann aber (auch) zur Client-Authentifikation in seinem Web-Browser verwenden kann. So wäre eine bürgerkartenlose Anmeldung am Web-Interface des Zustelldienstes möglich. Auch hier erfolgt die Abholung bzw. die Feststellung des Zustellnachweises im Wege der SSL-Client-Authentifizierung des Browsers. Anstelle der Bürgerkarte kann analog nach dem in Abschnitt 2.2 beschrieben Ansatz verfahren werden.

Darüberhinaus kann eine weiterführende Variation des automatisierten Abholens vorgesehen und angeboten werden, bei der der Zustelldienst nach Anmeldung des Empfängers am Web-Interface – unter Verwendung seines Client-Zertifikates – ein „Keep-Alive“-Browserfenster öffnet, welches durch laufendes wiederverbinden (periodisches Reload; durch aktiven Inhalt realisiert) eine laufende Annahme von Zustellstücken erwirkt (vgl. Lösungen zum Offenhalten von Sessions in kommerziellen WLANs). Die Laufende Annahme von Zustellstücken ergibt sich durch periodische Client-Authentifizierungen (SSL-Handshakes). Bei einer derartigen Lösung ist aber technisch dafür Sorge zu tragen, dass kein Wiederaufgriff bestehender SSL-Sessions erfolgt (Reuse), sondern ein tatsächliches SSL-Handshake erzwungen wird. Nur ein voller SSL-Handshake mit der dabei durchgeführten elektronischen Signatur erfüllt die Anforderungen einer automatisiert ausgelösten Signatur und kann als technisches Ersatzverfahren zur Annahme von Zustellstücken angesehen werden.

Die in diesem Dokument beschriebene Methode verwendet E-Mail Technologien bzw. Webbasierte Authentifizierung mittels Client-Zertifikat in Browsern. Zustelldienstbetreibern steht es frei, alternative Abholmöglichkeiten gemäß § 35(3) Zustellgesetz zur Verfügung zu stellen. Ein mögliche Alternative für eine automatisierte Abholung wären Web Service Technologien basierend auf HTTP und SOAP (Simple Object Access Protocol).

A. Revision History

Version	Datum	Autor(en)	
1.0.0	13.11.2007	Thomas Rössler (EGIZ) Reinhard Posch (BKA)	Erstellt
1.0.1	14.11.2007	Thomas Rössler (EGIZ) Reinhard Posch (BKA)	Klarstellung des Bezugs auf Novell. Ergänzungen zu Zertifikatsausstellung
1.0.2	17.12.2007	Thomas Rössler (EGIZ)	Klarstellung alternativer Abholmechanismen
1.3.0	17.03.2008	Thomas Rössler (EGIZ)	Umformatierung auf Konventions-Style keine inhaltlichen Änderungen Anpassung Versionsnummer zu ZUSE-Suite 1.3.0
1.4.0	24.01.2012	Arne Tauber (EGIZ)	Anm. weitere alt. Abholmöglichkeiten Ausstellungsvariante 3 (Fingerprint) Anpassung Versionsnummer zu ZUSE-Suite 1.4.0

B. Referenzen

[ZustG07]	Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz – ZustG), idF BGBl. I Nr. 5/2008.
[SigG07]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 idF. BGBl. I Nr. 8/2008.
[SigV07]	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV), BGBl. II Nr. 3/2008.